Distributed and Self-organizing Systems

SSE | Tutorial 6

Task 1

Complete the implementation of *MetadataReader.cs* in project *Task1-Template.zip*, which should be able to read metadata using WS-MetadataExchange from a given endpoint (e.g. http://pauline.informatik.tu-chemnitz.de/WcfAddService/Service1.svc/mex) [1]. Print content of all *MetadataSection*-elements to the console. For help you can consider *MetadataResponse.xml* within *Task1-Template.zip*.

Task 2

1. Record the traffic between a client from the project *WcfAddClient.zip* and the Web service from exercise 1. The communication requires encryption using the server's public key (from *wcfaddservice.p12*). Import the provided server certificate before starting the project (Double click on the file → Next →Next → Password: 1111 →Automatically select... → Next → Finish)
2. Use e.g. Wireshark[2] or Fiddler[3] to record the traffic between the client and the service. Which standards (besides SOAP) have you recognized in the request/response messages? What are they used for?

Task 3

Inform yourself about XML Encryption and Signature[4]. The bundle *XMLSec.zip* contains a command tool for signing and encrypting XML files[5]. Using the given private key *userkey.pem* (password: hello) decrypt the file *doc-encrypted.xml*. Using the given public key *pub-userkey.pem* check if its signature is correct. Upload the message inside the file using the template *exercise2.doc*:

Message	**Signature correct?**

Homework

Create an XML file, sign and encrypt it using the private key from the exercise 2. Test if you can decrypt it and verify the signature. Upload the encrypted file to OPAL.

[1] Accessible only from the university network

[2] http://www.wireshark.org/

[3] http://www.fiddler2.com/fiddler2/

[4] http://users.dcc.uchile.cl/~pcamacho/tutorial/web/xmlsec/xmlsec.html

[5] http://www.aleksey.com/xmlsec/